A Good Method of Combining Codes

Robert Calderbank
California Institute of Technology
Pasadena, California 91125

Submitted by Richard A. Brualdi

ABSTRACT

Let q be an odd prime power, and suppose $q \equiv -1 \pmod 8$, Let $C(q)$ and $C(q)^*$ be the two extended binary quadratic residue codes (QR codes) of length $q+1$, and let

$$T(q) = \{(a+x; b+x; a+b+x) : a, b \in C(q), x \in C(q)^*\}.$$

We establish a square root bound on the minimum weight in $T(q)$. Since the same type of bound applies to $C(q)$ and $C(q)^*$, this is a good method of combining codes.

INTRODUCTION

We shall denote the vector space $\mathrm{GF}(2)^n$ by $V_n(2)$. We shall sometimes denote the zero vector by $\mathbf{0}$ and the all-one vector by $\mathbf{1}$. A binary code is a subspace of $V_n(2)$. The weight $\mathrm{wt}(a)$ of a vector $a \in V_n(2)$ is the number of nonzero entries. An automorphism of a code C is a permutation matrix P such that $CP = C$. The automorphisms of C form a group, which we shall denote by $\mathrm{Aut}(C)$.

Throughout this paper q is an odd prime power satisfying $q \equiv -1 \pmod 8$. The extended binary QR code $C(q)$ is that subspace of $V_{q+1}(2)$ spanned by the rows of the matrix A given below. We have used the elements of the projective line $\mathrm{GF}(q) \cup \{\infty\}$ to index the rows and columns of this matrix:

$$A = \begin{array}{c} \\ \infty \\ \mathrm{GF}(q) \end{array} \begin{array}{c} \begin{array}{cc} \infty & \quad \mathrm{GF}(q) \end{array} \\ \left[\begin{array}{c|ccc} 1 & 1 & \cdots & 1 \\ \hline 1 & & & \\ \vdots & & B & \\ 1 & & & \end{array}\right] \end{array},$$

 0024-3795/80/040115+10$01.75

where

$$(B)_{ij} = \begin{cases} 1 & \text{if } j-i \text{ is a nonzero square,} \\ 0 & \text{otherwise.} \end{cases}$$

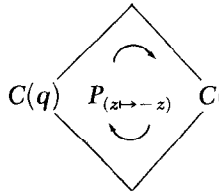
If π is a permutation of the set $\mathrm{GF}(q) \cup \{\infty\}$, then P_π denotes the permutation matrix corresponding to π.

We define $C(q)^* = C(q)P_{(z \mapsto -z)}$. Note that $q \equiv -1 \pmod 4$ and so -1 is a nonsquare in $\mathrm{GF}(q)$. The codes $C(q)$ and $C(q)^*$ are both invariant under the group G of matrices P_π where

$$\pi = \left(z \mapsto \frac{az^\sigma + b}{cz^\sigma + d}\right).$$

with $a, b, c, d \in \mathrm{GF}(q)$, $ad - bc$ a nonzero square, and σ an automorphism of $\mathrm{GF}(q)$. Figure 1 describes some more properties of $C(q)$ and $C(q)^*$. The codes $C(q)$ and $C(q)^*$ are both self-dual and all weights in each code are divisible by 4. For a proof of the next theorem we refer the reader to [4].

$$C(q) + C(q)^* = \{w \in V_{q+1}(2) : 2 \mid wt(w)\}$$



$$\dim C(q), C(q)^* = \frac{q+1}{2}$$

$$C(q) \cap C(q)^* = \langle \mathbf{1} \rangle$$

FIG. 1.

THEOREM. *Let d be a minimum weight in $C(q)$ (or $C(q)^*$). Then*

$$(d-1)^2 - (d-1) + 1 \geqslant q.$$

By definition

$$T(q) = \{(a+x; b+x; a+b+x) : a, b \in C(q),\ x \in C(q)^*\}.$$

Setting $A^* = AP_{(z \mapsto -z)}$, we see that $T(q)$ is that subspace of $V_{3q+3}(2)$ spanned

by the rows of the matrix

$$K=\left[\begin{array}{c|c|c} A & 0 & A \\ 0 & A & A \\ A^* & A^* & A^* \end{array}\right].$$

The two vertical lines split each vector into three components. Given that

$$[A,0,A]+[0,A,A]=[A,A,0],$$

we see that any permutation of the components is an automorphism of the code. If $M \in G$, *then the matrix*

$$\begin{bmatrix} M & & 0 \\ & M & \\ 0 & & M \end{bmatrix}$$

is an automorphism of $T(q)$. *Thus* $T(q)$ *is invariant under the group* $\mathfrak{R}$, *isomorphic to* $G \times S_3$, *generated by the automorphisms given above.*

The code $T(q)$ is visibly self-dual. Since all weights in $C(q)$ and $C(q)^*$ are divisible by 4, every row of the matrix K has weight divisible by 4. Since $T(q)$ is self-orthogonal, a standard inductive argument reveals that any sum of the rows of K has weight divisible by 4. Thus all weights in $T(q)$ are divisible by 4. The next theorem characterizes $T(q)$ in terms of $C(q)$ and $C(q)^*$. The proof is easy and we omit the details.

THEOREM. *Given* $f_1,f_2,f_3 \in V_{q+1}(2)$, *then* $(f_1;f_2;f_3) \in T(q)$ *if and only if*

(1) $f_i+f_j \in C(q)$ *for* $i,j=1,2,3$, *and*
(2) $f_1+f_2+f_3 \in C(q)^*$.

In 1967, R. J. Turyn [1] showed that $T(7)$ is the extended binary Golay code. In 1974, W. Feit [3] showed that $T(23)$ has minimum weight 12 and that $T(31)$ has minimum weight 16. This method of combining codes was also investigated by N. J. A. Sloane, S. M. Reddy, and C. L. Chen in [8]. The purpose of this paper is to prove the following theorem.

THEOREM. *If* d *is the minimum weight in* $T(q)$, *then*

$$(d-1)^2-(d-1)+7 \geqslant 3q.$$

This bound is analogous to the bound on the minimum weight in $C(q)$. One corollary of this theorem is that $T(7)$ is the extended binary Golay code. This is because V. Pless [6] has shown that this code is the unique self-dual binary code of length 24 and minimum weight 8.

THE MAIN THEOREM

Let

$$V=(a_\infty,\ldots,a_i,\ldots;b_\infty,\ldots,b_i,\ldots;c_\infty,\ldots,c_i,\ldots)$$

be a vector in $T(q)$. Let

$$d_1=|\{i\in \mathrm{GF}(q) \text{ such that } a_i\neq 0\}|,$$

$$d_2=|\{i\in \mathrm{GF}(q) \text{ such that } b_i\neq 0\}|,$$

$$d_3=|\{i\in \mathrm{GF}(q) \text{ such that } c_i\neq 0\}|.$$

Since $T(q)$ is self-orthogonal and since $(\mathbf{1};\mathbf{0};\mathbf{0})$, $(\mathbf{0};\mathbf{1};\mathbf{0})$, and $(\mathbf{0};\mathbf{0};\mathbf{1})$ are vectors in $T(q)$, we have

$$a_\infty=\sum_{i\in \mathrm{GF}(q)} a_i, \qquad b_\infty=\sum_{i\in \mathrm{GF}(q)} b_i, \quad \text{and} \quad c_\infty=\sum_{i\in \mathrm{GF}(q)} c_i. \tag{1.1}$$

Since $v\in T(q)$, we have $v=(f+h;g+h;f+g+h)$ where $f,g\in C(q)$ and $h\in C(q)^*$. If $f+h=\mathbf{0}$, then $f,h\in C(q)\cap C(q)^*$. It follows that $v=(\mathbf{0};g;g)$ or $v=(\mathbf{0};1+g;g)$. If $d=\mathrm{wt}(v)$, then $d\geqslant 2e$, where e is the minimum weight in $C(q)$. The square root bound on the minimum weight in $C(q)$ gives

$$\left(\frac{d}{2}-1\right)^2-\left(\frac{d}{2}-1\right)+1\geqslant q.$$

The next two lemmas follow directly from the action of $\mathfrak{N}$ on the coordinate positions.

LEMMA 1. *Let v, as above, be a vector of minimum weight in $T(q)$. Then we may choose v so that either*

(1) $a_\infty=b_\infty=c_\infty=1$, *or*
(2) $a_\infty=b_\infty=1$ *and* $c_\infty=0$, *or*
(3) $a_\infty=1, b_\infty=c_\infty=0$, *and no two components of v have a nonzero entry in the same position.*

LEMMA 2. *Let $v \in T(q)$ be a vector of weight d. If one component of v is zero, then*

$$(d-2)^2 - 2(d-2) + 4 \geqslant 4q.$$

Define $T(q)^* = T(q)\phi_1$, where

$$\phi_1 = \begin{bmatrix} P_{(z \mapsto -z)} & & 0 \\ & P_{(z \mapsto -z)} & \\ 0 & & P_{(z \mapsto -z)} \end{bmatrix}.$$

Note that $q \equiv -1 \pmod 4$ and so -1 is a nonsquare in GF(q).

LEMMA 3. *The subspaces $T(q)$ and $T(q)^*$ have the properties described in Fig. 2.*

Moreover, $T(q)^*$ is invariant under $\mathfrak{R}$.

$$T(q) + T(q)^* = \{(a;b;c) : 2 \mid \mathrm{wt}(a),\ 2 \mid \mathrm{wt}(b), \text{ and } 2 \mid \mathrm{wt}(c)\}$$

$$T(q) \quad \phi_1 \quad T(q)^* \qquad \dim T(q), T(q)^* = \frac{3q+3}{2}$$

$$T(q) \cap T(q)^* = \langle (\mathbf{1};\mathbf{0};\mathbf{0}), (\mathbf{0};\mathbf{1};\mathbf{0}), (\mathbf{0};\mathbf{0};\mathbf{1}) \rangle$$

FIG. 2.

Proof. Since ϕ_1 normalizes $\mathfrak{R}$ and since $T(q)^*$ is invariant under $\phi_1^{-1}\mathfrak{R}\phi_1$, it follows that $T(q)^*$ is invariant under $\mathfrak{R}$. Now $(\phi_1)^2 = I_{3q+3}$, and so the matrix ϕ_1 interchanges the two codes. Since $T(q)^*$ is also self-dual, we must have $T(q) \cap T(q)^* \perp (T(q) + T(q)^*)$. Since $(\mathbf{1};\mathbf{0};\mathbf{0})$, $(\mathbf{0};\mathbf{1};\mathbf{0})$, and $(\mathbf{0};\mathbf{0};\mathbf{1})$ are all in $T(q) \cap T(q)^*$, we must have

$$T(q) + T(q)^* \subseteq \{(a;b;c) : 2 \mid \mathrm{wt}(a),\ 2 \mid \mathrm{wt}(b), \text{ and } 2 \mid \mathrm{wt}(c)\}. \tag{1.2}$$

From Fig. 1 we know there exist $f \in C(q)$ and $g \in C(q)^*$ such that $\mathrm{wt}(f+g) = 2$. Now

$$\{(f;\mathbf{0};f) + (g;g;g)\} + \{(g;\mathbf{0};g) + (f;f;f)\} = (\mathbf{0};f+g;\mathbf{0})$$

is a vector of weight 2 in $T(q)+T(q)^*$. The sum $T(q)+T(q)^*$ is $\mathfrak{R}$-invariant. From the action of $\mathfrak{R}$ on the coordinate positions we conclude that equality holds in (1.2). An easy dimension argument completes the proof. ■

Let R and R^* be those subspaces of $V_{3q}(2)$ obtained from $T(q)$ and $T(q)^*$ by taking each codeword and deleting the three entries indexed by ∞. Let ϕ be the matrix obtained from ϕ_1 by deleting the three rows and columns indexed by ∞. The next lemma follows immediately from Lemma 3.

LEMMA 4. *The subspaces R and R^* have the properties described in Fig. 3.*

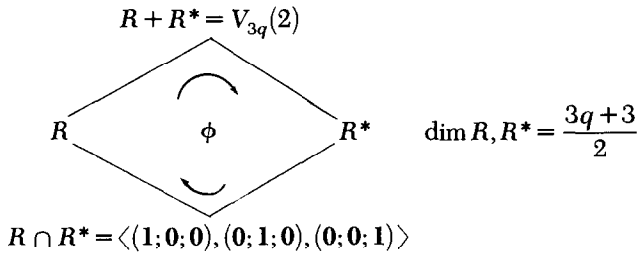


FIG. 3.

If

$$Q_i=\begin{bmatrix} P_i & & 0 \\ & P_i & \\ 0 & & P_i \end{bmatrix} \quad \text{and} \quad \tau=\begin{bmatrix} 0 & I_q & 0 \\ 0 & 0 & I_q \\ I_q & 0 & 0 \end{bmatrix},$$

where $P_i=P_{(z\mapsto z+i)}$ $[z\in \mathrm{GF}(q)]$, then the subspaces R and R^* are both invariant under the group $Q=\langle \tau, Q_i : i\in \mathrm{GF}(q)\rangle$.

The map

$$\varphi:(\ldots,a_i,\ldots;\ldots,b_i,\ldots;\ldots,c_i,\ldots)\mapsto$$

$$\sum_{i\in \mathrm{GF}(q)} a_iQ_i+\tau\sum_{i\in \mathrm{GF}(q)} b_iQ_i+\tau^2\sum_{i\in \mathrm{GF}(q)} c_iQ_i$$

is a vector space isomorphism between $V_{3q}(2)$ and the GF(2)-algebra A spanned by the matrices in Q. Since $\tau Q_i=Q_i\tau$ for all $i\in \mathrm{GF}(q)$, we have

$$\{\Sigma a_iQ_i+\tau\Sigma b_iQ_i+\tau^2\Sigma c_iQ_i\}\tau=\Sigma c_iQ_i+\tau\Sigma a_iQ_i+\tau^2\Sigma b_iQ_i$$

and

$$\left\{\Sigma a_i Q_i + \tau \Sigma b_i Q_i + \tau^2 \Sigma c_i Q_i\right\} Q_j = \Sigma a_i Q_{i+j} + \tau \Sigma b_i Q_{i+j} + \tau^2 \Sigma c_i Q_{i+j}.$$

It follows that φ is an A-module homomorphism and that the subspaces R and R^* correspond to ideals in A. We also note that substitution

$$(\Sigma a_i Q_i) \mapsto (\Sigma a_i)$$

is a GF(2)-algebra homomorphism between A and GF(2).

THEOREM 4. *If d is the minimum weight in $T(q)$, then*

$$(d-1)^2 - (d-1) + 7 \geqslant 3q.$$

Proof. Let v be a vector of minimum weight d in $T(q)$ satisfying the conclusions of Lemma 1. By Lemma 2 we may assume that no component of v is zero. Deleting the entries a_∞, b_∞, and c_∞ gives a vector $w \in R$ such that

$$w = \Sigma a_i Q_i + \tau \Sigma b_i Q_i + \tau^2 \Sigma c_i Q_i.$$

Since $w(w\phi) \in RR^*$ and since $RR^* \subseteq R \cap R^*$, we have

$$\begin{aligned} w(w\phi) &= \left(\Sigma a_i Q_i + \tau \Sigma b_i Q_i + \tau^2 \Sigma c_i Q_i\right) \\ &\quad \times \left(\Sigma a_i Q_{-i} + \tau \Sigma b_i Q_{-i} + \tau^2 \Sigma c_i Q_{-i}\right) \\ &= k_1 \Sigma Q_i + k_2 \tau \Sigma Q_i + k_3 \tau^2 \Sigma Q_i. \end{aligned} \tag{1.3}$$

Applying the substitution map gives

$$qk_1 = (\Sigma a_i)^2 + 2(\Sigma b_i)(\Sigma c_i),$$

$$qk_2 = (\Sigma c_i)^2 + 2(\Sigma a_i)(\Sigma b_i),$$

$$qk_3 = (\Sigma b_i)^2 + 2(\Sigma a_i)(\Sigma c_i).$$

By (1.1) these equations simplify to

$$k_1 = a_\infty, \qquad k_2 = c_\infty, \quad \text{and} \quad k_3 = b_\infty. \tag{1.4}$$

We now count distinct nonzero coefficients in (1.3):

$$\text{if} \quad k_1 = 1, \quad \text{then} \quad d_1^2 - d_1 + 1 + 2d_2d_3 \geqslant q, \tag{1.5}$$

$$\text{if} \quad k_2 = 1, \quad \text{then} \quad d_3^2 - d_3 + 1 + 2d_1d_2 \geqslant q, \tag{1.6}$$

$$\text{if} \quad k_3 = 1, \quad \text{then} \quad d_2^2 - d_2 + 1 + 2d_1d_3 \geqslant q. \tag{1.7}$$

By Lemma 1 we can split the proof into three cases.

Case 1: $a_\infty = b_\infty = c_\infty = 1$. By (1.4), $k_1 = k_2 = k_3 = 1$, and adding together (1.5), (1.6), and (1.7) gives

$$(d_1 + d_2 + d_3)^2 - (d_1 + d_2 + d_3) + 3 \geqslant 3q.$$

Since $d_1 + d_2 + d_3 = d - 3$, we have

$$(d-3)^2 - (d-3) + 3 \geqslant 3q,$$

and the theorem is proven.

Case 2: $a_\infty = 1$, $b_\infty = c_\infty = 0$, *and no two components of* v *have a nonzero entry in the same position.* By (1.4), $k_1 = 1$ and so (1.5) holds. Let c_j be a nonzero entry in v, and let $M \in \mathfrak{N}$ be an automorphism interchanging the indices j and ∞. Then

$$vM = (0, f; 0, g; 1, h),$$

where $\mathrm{wt}(f) = d_1 + 1$, $\mathrm{wt}(g) = d_2$, and $\mathrm{wt}(h) = d_3 - 1$. The analogue of (1.6) for vM gives

$$(d_3 - 1)^2 - (d_3 - 1) + 1 + 2(d_1 + 1)d_2 \geqslant q. \tag{1.8}$$

An identical argument shows

$$(d_2 - 1)^2 - (d_2 - 1) + 1 + 2(d_1 + 1)d_3 \geqslant q. \tag{1.9}$$

Adding together (1.5), (1.8), and (1.9) gives

$$(d_1+d_2+d_3)^2-(d_1+d_2+d_3)+7\geqslant 3q.$$

Since $d_1+d_2+d_3=d-1$, we have

$$(d-1)^2-(d-1)+7\geqslant 3q.$$

Case 3: $a_\infty=b_\infty=1$ *and* $c_\infty=0$. By (1.4), $k_1=k_3=1$ and so (1.5) and (1.7) hold. If the first two components of v are identical, then $v=(f+h;f+h;h)$, where $f\in C(q)$ and $h\in C(q)^*$. Since $h\neq 0$, the square root bound on the minimum weight in $C(q)^*$ gives

$$(d_3-1)^2-(d_3-1)+1\geqslant q. \tag{1.10}$$

If the first two components of v are not identical, then we may suppose there exists $j\in \mathrm{GF}(q)$ such that $b_j=1$ and $a_j=0$. There is no loss of generality; a similar argument would apply if we had $b_j=0$ and $a_j=1$. Let $M\in\mathfrak{N}$ be an automorphism interchanging the indices j and ∞. Deleting the three entries of vM indexed by ∞ gives a vector $y\in R$ such that

$$y=\Sigma f_iQ_i+\tau\Sigma g_iQ_i+\tau^2\Sigma h_iQ_i.$$

Since $w(y\phi)\in R\cap R^*$, we have

$$w(y\phi)=k_4\Sigma Q_i+k_5\tau\Sigma Q_i+k_6\tau^2\Sigma Q_i, \tag{1.11}$$

and applying the substitution map gives

$$k_5=(\Sigma a_i)(\Sigma g_i)+(\Sigma b_i)(\Sigma f_i)+(\Sigma c_i)(\Sigma h_i).$$

By (1.1) we have

$$\Sigma a_i=1,\quad \Sigma g_i=1,\quad \Sigma f_i=0,\quad \text{and}\quad \Sigma c_i=0,$$

and it follows that $k_5=1$. Counting nonzero coefficients in (1.11) gives

$$d_3^2+d_1d_2+d_2(d_1+1)\geqslant q. \tag{1.12}$$

Adding (1.5) and (1.7) to one of (1.10) and (1.12) gives

$$(d_1+d_2+d_3)^2-d_1+2\geqslant 3q.$$

Since $d_1+d_2+d_3=d-2$ and since $d_1\geqslant 2$, we have

$$(d-2)^2\geqslant 3q,$$

and the theorem is proven. ■

REMARK. The author has used similar techniques to establish a square root bound on the minimum weight of the ternary symmetry codes constructed by V. Pless and the quasicyclic binary codes constructed by V. K. Bhargava, S. E. Tavares, and S. G. S. Shiva [2].

REFERENCES

1 E. F. Assumus, Jr., H. F. Mattson, Jr., and R. J. Turyn, Research to develop the algebraic theory of codes, Air Force Cambridge Res. Lab., Bedford, Mass., Sci. Rep. AFCRL-67-0365, 1967.

2 V. K. Bhargava, S. E. Tavares, and S. G. S. Shiva, Difference sets of the Hadamard type and quasi-cyclic codes, *Information and Control* 26:341–350 (1974).

3 W. Feit, A self-dual even (96,48,16) code, *IEEE Trans. Information Theory* IT-20:136–138 (1974).

4 J. H. van Lint and F. J. MacWilliams, Generalized quadratic residue codes, *IEEE Trans. Information Theory* IT-24:730–737 (1978).

5 F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1978.

6 V. Pless, On the uniqueness of the Golay codes, *J. Combinatorial Theory* 5:215–228 (1968).

7 V. Pless, Symmetry codes over GF(3) and new five-designs, *J. Combinatorial Theory* 12:119–142 (1972).

8 N. J. A. Sloane, S. M. Reddy, and C. L. Chen, New binary codes, *IEEE Trans. Information Theory* IT-18:503–510 (1972).

Received 17 July 1979; revised 21 September 1979